REMARKS

Claims 1 – 31 are pending in the application.

Claim Rejections – 35 USC 103

Claims 1 – 8, 13 – 16 and 21 - 27 were rejected under 35 USC 103(a)as being unpatentable over Kunstadt US 5,003,598 in view of Shefi US 6,266,413. Favorable reconsideration of this rejection is respectfully requested since, as will be shown below, Kunstadt and Shefi when combined do not teach the present invention as claimed in claim 1.

Kunstadt teaches encrypted communication between two parties over a mobile telephone link using a second *unconnected analog* signal available to both of the parties in order to encrypt and decrypt their communication in real time. The second unconnected analog signal is referred to in column 2 line 32 as a "public signal". It is referred to again in column 2 line 54 as the "broadcast signal." That is to say, what Kunstadt teaches is using a publicly broadcast analog radio signal and its audio output to encrypt the cellular communication between the two parties.

The Examiner states that Kunsdadt teaches a digital bitstream because mobile telephony uses digital signals. However it is respectfully pointed out that Kunstadt clearly teaches encoding of an *analog* signal. With reference to Figure 2 of Kunsdtadt, the signal is input at input 28 and fed to rectifier 39 and then low pass filter 36 before being amplified at amplifier 37. It will be clear that operations of rectification and amplification are analog operations and are only possible with an analog input. They *could not be carried out* with a digital bitstream.

Furthermore, and more significantly, the actual encoding and decoding processes as taught by Kunsdadt, are analog processes in themselves. The processes

include adding pseudo-random noise to the pure voice signal based on a filtered and thresholded version of the analog signal together with an element from the public broadcast signal, all compounded together using mixer 32. It will be appreciated that such a clearly analog process using analog components cannot be performed on a digital bitstream.

It is pointed out that in the system of Kunsdadt, the communication signal is public and the random data source is public. The secret held by the two parties is the setting of eight manually settable switches 53, which give a starting point.

The Examiner then cites Shefi. Shefi teaches a secret table that each of the parties have, with an exchange of starting numbers that allow each party to inspect the look-up table. Essentially the exchange of numbers provides addresses in the lookup table, and therefore constitutes a selector for looking up a table in order to encode a third element which is the communication or message.

That is to say Shefi teaches a three element system, a message, a table and a selector, of which the table is secret and the message and selectors are public.

It would not be obvious to combine Shefi with Kunstadt since the two systems are incompatible. Kunstadt uses a first analog signal to scramble a second analog signal. It has no meaning to look up addresses in the context of analog signals, since analog signals have to be sampled and cannot be looked up. Therefore it makes no sense to apply the selector signals of Shefi to Kunsdadt, since there is no way that they can be used to look up the analog signal.

Secondly, even if the selector signal of Shefi were supplied to Kunsdadt, the selector signals of Shefi are public, and the looked up signal of Kunsdadt is public. Therefore the result of combining the two systems would be to use a public signal to look up a public signal. The skilled person would be led away from making such a

combination due to the clear lack of utility. The starting switches of Kunstadt which set analog voltage levels would be of no assistance in setting the selector of Shefi which does not rely on analog voltage levels.

The two systems of Kunsdatd and Shefi are thus completely incompatible. Kunsdadt teaches analog scrambling of an analog signal, and Shefi teaches digital selecting of addresses in a secret table to produce a one-time pad that can be used for encryption. Not only do the two systems not combine to provide the system of claim 1, but the two systems of Kunsdadt and Shefi could not be combined even in principle.

Even if the two systems were combined, they do not in combination teach using the actual communication transmission between the two parties to seed the encryption process as required by the present claims.

By contrast the present invention provides *a digital bitstream* which is available to both parties, and a random selector which uses data from *the bitstream itself* to generate a random bit source.

By contrast with the cited prior art, there is no need for a commonly held table as in Shefi, and there is no need for a publicly transmitted signal separate from the exchanged signal as in Kunstadt. The prior art does not know how to provide a random bit source available at both the parties without providing an entire secret table which is available separately and identically at each party as in Shefi. It will be appreciated by the Examiner, that the need for such a table at each party makes secret communication possible only if serious preparations were made beforehand. Yet the prior art has no solution to this issue.

Thus independent claims 1, 13 and 21 are believed to be novel and inventive for the above reasons. The remaining claims are believed to be allowable as being dependent on allowable main claims.

All of the matters raised by the Examiner have been dealt with and are believed to have been overcome. In view of the foregoing, it is respectfully submitted that all the claims now pending in the application are allowable over the cited reference. An early Notice of Allowance is therefore respectfully requested.

Respectfully submitted,

Sol Sheinbein
Registration No. 25,457

Date: February 9, 2005